S/N: 10/059,099

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 788 649**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **99 00462**

(51) Int Cl^7 : **H 04 L 9/00**, G 06 K 19/07

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 18.01.99.

(30) **Priorité** :

(43) **Date de mise à la disposition du public de la demande** : 21.07.00 Bulletin 00/29.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *SCHLUMBERGER SYSTEMES* *Société anonyme* — FR.

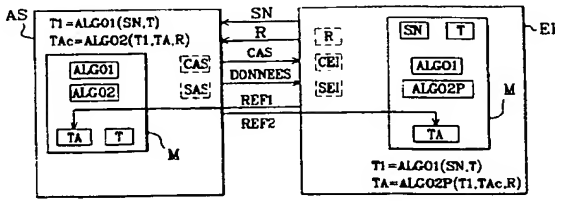
(72) **Inventeur(s)** : BUTNARU DAN, GELZE MATHIAS et ROSSET RAPHAEL.

(73) **Titulaire(s)** :

(74) **Mandataire(s)** : SCHLUMBERGER SYSTEMES.

(54) PROCEDE DE CHARGEMENT SECURISE DE DONNEES ENTRE DES MODULES DE SECURITE.

(57) L'invention concerne un procédé de chargement sécurisé d'une clef applicative à partir d'un premier module de sécurité vers un ou plusieurs deuxièmes modules de sécurité, lesdits premier et deuxièmes modules comprenant chacun au moins une mémoire. L'invention se caractérise en ce que ledit procédé comporte des étapes selon lesquelles, lors de chaque chargement, on calcule dans le premier et deuxièmes modules une clef d'exploitation, ladite clef est utilisée pour le chiffrement dans le premier module de la clef applicative. Cette dernière est par la suite envoyée au deuxième module, déchiffrée et vérifiée dans ledit module. La clef d'exploitation n'est pas enregistrée dans la mémoire des modules de sécurité. L'invention s'applique, en particulier, à la personnalisation de modules de sécurité.



FR 2 788 649 - A1

PROCEDE DE CHARGEMENT SECURISE DE DONNEES ENTRE DES MODULES DE SECURITE

La présente invention concerne un procédé de chargement sécurisé d'une clef applicative à partir d'un premier module de sécurité vers un ou plusieurs deuxièmes modules de sécurité, lesdits premier et deuxièmes modules comprenant chacun au moins une mémoire.

L'invention trouve une application particulièrement avantageuse lors d'une phase de personnalisation de deuxièmes modules de sécurité. Cette phase de personnalisation est effectuée avant une phase d'utilisation desdits deuxièmes modules. Par exemple, lors d'une phase d'utilisation dans le domaine de la fidélité, les deuxièmes modules se trouvent dans des terminaux de stations service et sont utilisés de manière à fournir des prestations de sécurisation de transactions de débit-crédit de points de fidélité entre un desdits terminaux et des cartes de crédit d'utilisateurs.

Le premier module ainsi que les deuxièmes modules de sécurité comportent une clef de transport et au moins une clef applicative dans leur mémoire. Les deuxièmes modules comportent également une clef dite d'exploitation et des informations de diversification qui permettent de différencier lesdits modules entre eux. Ladite clef applicative est utilisée afin de pouvoir utiliser les deuxièmes modules lors d'une phase d'utilisation et est à cette fin chargée dans lesdits modules à partir du premier module de sécurité lors de la phase de personnalisation. Les clefs de transport et d'exploitation ainsi que les informations de diversification sont utilisées pour sécuriser ledit chargement.

En vue de charger ladite clef applicative dans un deuxième module, l'état de la technique propose des procédés qui comportent des étapes consistant à :

- calculer la clef d'exploitation à partir de la clef de transport dudit deuxième module et de ses informations de diversification,

- remplacer ladite clef de transport par ladite clef d'exploitation dans ledit deuxième module en enregistrant ladite clef d'exploitation dans ledit module, c'est à dire en inscrivant ladite clef dans la mémoire dudit module de façon permanente,
- calculer, dans le premier module, la clef d'exploitation à partir de la clef de transport dudit premier module et des informations de diversification du deuxième module,
- charger la clef applicative provenant du premier module dans le deuxième module en utilisant les informations de diversification dudit module, la clef d'exploitation enregistrée dans le deuxième module et celle calculée dans le premier module ainsi que des algorithmes de cryptage et de décryptage.

Bien que ces procédés permettent un chargement sécurisé d'une clef applicative d'un premier module de sécurité vers un deuxième module de sécurité, ils nécessitent un enregistrement préalable d'une clef d'exploitation dans chacune des mémoires des deuxièmes modules qui demeure dans lesdits modules en fin de phase de personnalisation et lors de la phase d'utilisation et ce de façon permanente. Cela rend lesdits modules vulnérables dans la mesure où un fraudeur, pendant les deux phases précitées, peut découvrir ladite clef d'exploitation par des méthodes telles que la méthode connue des signatures électroniques desdits modules. De plus, lesdits procédés nécessitent de nombreuses opérations préalables pour effectuer le chargement d'une clef applicative, ce qui accroît le temps global de la phase de personnalisation.

Aussi, un problème technique à résoudre par l'objet de la présente invention est de proposer un procédé de chargement sécurisé d'une clef applicative à partir d'un premier module de sécurité vers un ou plusieurs deuxièmes modules de sécurité, lesdits premier et deuxièmes modules comprenant chacun au moins une mémoire, qui permettrait, d'une part, d'éviter à un fraudeur de découvrir une clef

d'exploitation, et, d'autre part, de gagner du temps lors de la phase de personnalisation des modules de sécurité.

Une solution au problème technique posé se caractérise en ce que ledit procédé de chargement comporte les étapes selon lesquelles :

- lors de chaque chargement, on calcule dans le premier module une clef d'exploitation à partir d'une information propre au deuxième module, d'une clef de transport et d'un algorithme de diversification, ladite clef de transport se trouvant dans le premier module de sécurité,
- on chiffre dans le premier module la clef applicative à partir d'informations comprenant ladite clef d'exploitation et d'un algorithme de cryptage,
- on envoie au deuxième module des données comprenant la clef applicative chiffrée,
- lors de chaque chargement, on calcule dans le deuxième module la clef d'exploitation à partir de l'information propre au deuxième module, de la clef de transport et de l'algorithme de diversification, ladite clef de transport se trouvant dans le module de sécurité, ladite clef d'exploitation n'étant pas enregistrée dans la mémoire dudit module,
- on déchiffre dans le deuxième module la clef applicative chiffrée, à partir d'informations comprenant ladite clef d'exploitation et d'un algorithme de décryptage inverse de l'algorithme de cryptage.

Ainsi, comme on le verra en détail plus loin, le procédé de chargement de l'invention permet, en calculant ladite clef d'exploitation et en ne la conservant que le temps du chiffrement ou du déchiffrement de la clef applicative, d'améliorer la sécurité du chargement d'une clef applicative. Il n'est en effet pas nécessaire d'enregistrer ladite clef d'exploitation dans les modules de sécurité. Les éventuelles fraudes sont par conséquent évitées et on n'effectue plus d'opérations qui sont

coûteuses en temps pour la phase de personnalisation, le temps de calcul de la clef d'exploitation étant infime par rapport au temps d'accès nécessaire à l'enregistrement de la clef d'exploitation.

La description qui va suivre au regard des dessins annexés, donnée à titre d'exemple non limitatif, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

La figure 1 est un schéma montrant un premier module et plusieurs deuxièmes modules.

La figure 2 est un schéma montrant le premier module et un deuxième module de la figure 1.

La figure 3 est un schéma montrant un échange de données entre le premier module et le deuxième module de la figure 2.

La figure 4 un schéma montrant un deuxième échange de données entre le premier module et le deuxième module de la figure 2.

La figure 5 est un schéma montrant un troisième échange de données entre le premier module et le deuxième module de la figure 2.

La figure 6 est un schéma montrant un quatrième échange de données entre le premier module et le deuxième module de la figure 2.

Sur la figure 1 est représenté un premier module AS de sécurité et plusieurs modules EI de sécurité, chaque module comprenant au moins une mémoire M. Selon l'objet de la présente invention, comme montré à la figure 2, le premier module AS ainsi que le deuxième module EI comportent une même clef T de transport et un même algorithme ALGO1 appelé algorithme de diversification qui se trouvent dans la mémoire M. En outre, le premier module AS comporte un ensemble de clefs applicatives TA et un algorithme ALGO2 de cryptage. Ces deux algorithmes peuvent être utiliser un même algorithme de base. Le module EI, quant à lui, comprend une information SN qui lui est propre.

Afin d'utiliser le deuxième module EI de sécurité, il faut au préalable charger une clef applicative TA du premier module AS lors

d'une phase dite de personnalisation comprenant plusieurs étapes décrites ci-après. Ladite clef est transférée par l'intermédiaire d'un réseau de communication.

Dans une première étape, lors de chaque chargement, on calcule dans le premier module AS une clef T1 d'exploitation à partir de l'information SN propre au deuxième module EI, de la clef T de transport et de l'algorithme ALGO1 de diversification, ladite clef T de transport se trouvant dans le premier module AS de sécurité comme décrit précédemment. L'information SN propre au deuxième module EI ne se trouve pas dans le premier module. Aussi, comme le montre la figure 3, on envoie au premier module AS l'information SN propre au deuxième module EI, préalablement au calcul dans le premier module AS de la clef T1 d'exploitation. Ladite clef T1 va servir au chargement d'une des clefs applicatives TA contenues dans le premier module AS, ladite clef applicative choisie sera chiffrée et envoyée au module EI.

Comme le montre la figure 3, pour choisir une desdites clefs applicatives TA, dans une deuxième étape, on envoie au premier module AS une information REF1 relative à ladite clef applicative TA, préalablement au chiffrement dans ledit module AS de la clef applicative TA. On choisit la clef applicative TA à chiffrer à partir de l'information REF1 relative à ladite clef applicative TA, préalablement au chiffrement dans le premier module AS de la clef applicative TA. On peut par exemple envoyer une référence représentant un numéro de clef ayant une valeur de trois pour indiquer que l'on choisit la troisième clef. C'est cette dernière qui est chargée dans le deuxième module EI. S'il n'existe pas de clef applicative TA référencée par ledit nombre REF1, le premier module AS indique que ladite clef n'existe pas.

Dans une troisième étape, comme le montre la figure 3, on chiffre dans le premier module AS la clef applicative TA à partir d'informations comprenant ladite clef T1 d'exploitation et de l'algorithme ALGO2 de cryptage. Après avoir chiffré ladite clef TA, on envoie au deuxième

module EI des données DONNEES comprenant la clef applicative TA chiffrée.

Dans une quatrième étape, on déchiffre dans le deuxième module EI la clef applicative TA chiffrée, à partir d'informations comprenant ladite clef T1 d'exploitation et d'un algorithme ALGO2P de décryptage inverse de l'algorithme ALGO2 de cryptage. Dans cette étape, afin de retrouver la clef applicative TA choisie, il est nécessaire d'utiliser la même clef T1 d'exploitation qui a été utilisée pour le cryptage de ladite clef applicative TA dans le premier module AS de sécurité. A cette fin, préalablement au déchiffrement de la clef applicative TA chiffrée, lors de chaque chargement, on calcule dans le deuxième module EI la clef T1 d'exploitation à partir de l'information SN propre au deuxième module EI, de la clef T de transport et de l'algorithme ALGO1 de diversification, ladite clef T de transport se trouvant dans le module EI de sécurité, ladite clef T1 d'exploitation n'étant pas enregistrée dans la mémoire M dudit module. Ledit calcul peut se faire à tout moment avant le déchiffrement de la clef. Les éléments nécessaires au calcul de cette clef T1 d'exploitation dans le deuxième module EI de sécurité sont les mêmes que ceux utilisés pour le calcul de la clef T1 d'exploitation dans le premier module AS. Par conséquent, les deux clefs T1 sont identiques et on retrouve bien dans le deuxième module EI la clef applicative TA choisie. Le fait de ne pas enregistrer une clef T1 d'exploitation dans une mémoire M d'un deuxième module EI rend une fraude plus difficile à effectuer dans la mesure où si un fraudeur veut trouver une clef applicative TA, il doit auparavant retrouver la clef T1 d'exploitation utilisée. Comme cette dernière clef n'est pas enregistrée dans le module cela rend les choses encore plus difficiles. De plus cela facilite la personnalisation et une mise sur le terrain d'un nième deuxième module EI dans la mesure où pour personnaliser les deuxièmes modules il n'est plus nécessaire d'effectuer deux chargements, un premier d'une clef T1 d'exploitation et un deuxième d'une clef

applicative TA, mais simplement un chargement d'une clef applicative TA. On se libère ainsi de du premier chargement qui est habituellement effectué par une entité différente du premier module AS, ce qui complique généralement d'autant plus les choses.

A l'instar du premier module AS, un module EI peut contenir une ou plusieurs clefs applicatives TA. Aussi, dans une cinquième étape, on envoie au deuxième module EI une information REF2 relative à une clef applicative TA, préalablement au déchiffrement dans ledit module EI de la clef applicative TA chiffrée, comme le montre la figure 4. Dans l'exemple précédent concernant le domaine de la fidélité, lors de l'utilisation d'un deuxième module EI, celui-ci doit pouvoir fournir différentes prestations telles que la sécurisation des transactions de débit-crédit de points pour par exemple différents types de carburant. Il est ainsi important d'avoir différentes clefs applicatives TA dans ledit module EI pour gérer la sécurisation de ces différents types de transactions. Le chargement de la clef applicative TA provenant du premier module AS peut ainsi permettre de charger une nouvelle clef applicative TA dans le deuxième module EI ou de modifier la valeur d'une clef TA déjà existante dans ledit deuxième module EI. L'information REF2 permet, soit de choisir la clef applicative TA qui va recevoir la valeur de la clef applicative provenant du premier module AS, soit d'indiquer un emplacement où sera chargée ladite clef TA provenant dudit premier module AS. Dans le cas où la clef applicative TA référencée par ladite information REF2 n'existe pas ou que ledit emplacement n'existe pas ou n'est pas fait pour acceuillir un clef, le deuxième module rejette la clef reçue et indique qu'une erreur s'est produite. Les informations REF1 et REF2 envoyées respectivement au premier et deuxième modules de sécurité peuvent être équivalentes. Une des clefs applicatives TA se trouvant dans le deuxième module EI est utilisée par ledit module pour s'identifier vis-à-vis d'entités extérieures comme par exemple une carte utilisateur. Or ladite

identification doit être unique. Par conséquent, ladite clef TA ne doit pas avoir de doublon. Aussi, lorsque l'on veut charger cette clef, on diversifie dans le premier module AS ladite clef applicative TA choisie, préalablement au chiffrement de ladite clef. La diversification se fait en fonction d'une information propre à chaque deuxième module.

Enfin, dans une dernière étape, on enregistre dans le deuxième module EI, après le déchiffrement de la clef applicative TA chiffrée, ladite clef TA dans ledit module EI. L'enregistrement dans ledit deuxième module EI de la clef applicative TA se fait en fonction de l'information REF2 relative à une clef applicative TA.

Le deuxième module EI peut maintenant être utilisé. On notera qu'aucune clef T1 d'exploitation n'a été transférée du premier module AS au deuxième module EI et n'a été enregistrée dans la mémoire M des modules de sécurité. Les opérations nécessaires à ces deux actions ne sont pas effectuées ce qui permet de gagner du temps lors de la phase de personnalisation. On ne mémorise pas une donnée secrète immédiatement utilisable par un algorithme ce qui évite à un fraudeur qui analyse ledit algorithme de découvrir ladite donnée. Enfin, il est inutile pour le fraudeur d'espionner soit le réseau de communication soit les modules de sécurité afin de trouver la clef T1 d'exploitation utilisée.

Un troisième avantage de l'objet de la présente invention se trouve dans le fait que l'information SN propre à chaque deuxième module EI de sécurité est unique. La clef T1 d'exploitation, qui est diversifiée c'est à dire calculée à partir de cette information, est par conséquent unique pour chaque module EI de sécurité. Par suite, la clef applicative TA chiffrée, qui est fonction de ladite clef T1 d'exploitation, n'est destinée qu'à un unique deuxième module EI destinataire ce qui renforce l'aspect sécuritaire de l'invention. Si un deuxième module EI n'a pas la même information SN que celle utilisée pour calculer la clef T1 d'exploitation dans le premier module AS et s'il reçoit ainsi une clef applicative TA qui

ne lui est pas destinée, il rejette ladite clef et indique qu'une erreur s'est produite.

D'autres aspects sécuritaires décrits ci-dessous sont couverts par l'objet de la présente invention.

L'objet de la présente invention prévoit une étape supplémentaire, montrée à la figure 4, selon laquelle on envoie au premier module AS un nombre aléatoire R issu du deuxième module EI, préalablement au chiffrement dans le premier module AS de la clef applicative TA. Les informations permettant, d'une part, de chiffrer la clef applicative TA dans le premier module AS, et, d'autre part, de déchiffrer dans le deuxième module EI la clef applicative TA chiffrée, comprennent le nombre aléatoire R issu du deuxième module EI. L'utilisation du nombre aléatoire R pour chiffrer et déchiffrer ladite clef applicative TA évite d'avoir une même valeur de chiffrement d'une clef applicative TA destinée à un deuxième module EI lorsque l'on charge plusieurs fois ladite clef dans ledit module. Le chiffrement d'une clef applicative TA destinée à un deuxième module EI est unique. Ainsi, un fraudeur qui espionne le réseau de communication et récupère les données DONNEES lors du transfert n'obtient jamais une même valeur de chiffrement et ne peut par conséquent découvrir un secret relatif à la clef applicative TA transférée.

Cependant, lors dudit transfert, le fraudeur peut avoir effectué des opérations frauduleuses qui altèrent les données transférées. Aussi, on vérifie que les données DONNEES comprenant la clef applicative TA chiffrée sont intègres. A cette fin, comme le montre la figure 5, on calcule dans le premier module AS un certificat CAS sur lesdites données DONNEES, préalablement á l'envoi desdites données, ledit certificat étant envoyé par la suite au deuxième module EI et vérifié dans ledit deuxième module, préalablement au déchiffrement dans ledit deuxième module EI de la clef applicative TA chiffrée. Afin d'effectuer la vérification, on calcule dans le deuxième module EI un certificat CEI en

fonction des données reçues et on compare les deux certificats CAS et CEI. Si une fraude ou une erreur s'est produite lors dudit transfert, la vérification du certificat CAS est erronée, le déchiffrement de la clef applicative TA ne se fait pas et le deuxième module EI indique qu'une erreur s'est produite. Ce système garantit ainsi une intégrité des données DONNEES lors de leur transfert depuis le premier module AS vers le deuxième module EI sur le réseau de communication.

De même qu'il faut garantir l'intégrité des données transférées, de même il faut garantir l'authenticité des données qui sont enregistrées dans le deuxième module EI. Ainsi, on vérifie que la clef applicative TA est authentique. A cet effet, comme le montre la figure 5, on calcule dans le premier module AS, préalablement au chiffrement de la clef applicative TA, une signature SAS de ladite clef TA, ladite signature étant envoyée par la suite au deuxième module EI et vérifiée dans ledit module. La vérification de la signature de ladite clef applicative TA se fait postérieurement au déchiffrement dans le deuxième module EI de ladite clef TA chiffrée et préalablement à l'enregistrement de ladite clef dans ledit module. Afin d'effectuer la vérification, on calcule dans le deuxième module EI une signature SEI avec la clef applicative TA déchiffrée dans ledit module EI et on compare les deux signatures SAS et SEI. Dans le cas où les deux signatures sont équivalentes, la clef applicative TA déchiffrée est authentique et est enregistrée. Dans le cas où la clef applicative TA n'est pas authentique, l'enregistrement de ladite clef ne se fait pas et le deuxième module EI indique qu'une erreur s'est produite. Le système décrit ci-dessus permet ainsi de vérifier que l'on récupère bien la clef applicative TA choisie dans le premier module AS et non une autre clef. On notera que lorsque ladite signature SAS existe, le certificat CAS est calculé également en fonction de ladite signature SAS. Ladite signature fait partie des données DONNEES envoyées lors de la troisième étape décrite précédemment.

L'envoi de données telles qu'un certificat ou une signature à un module de sécurité fait appel à des opérations dont le temps d'accomplissement s'ajoute à celui de la phase de personnalisation. Aussi, comme le montre la figure 6, afin de réduire le nombre d'accès aux différents modules et ainsi de réduire le temps de personnalisation, on envoie l'ensemble des données dont a besoin un module de sécurité en une seule fois au moyen d'une unique commande. Le nombre R aléatoire , le nombre REF1 relatif à une clef applicative TA et le nombre SN propre au deuxième module EI sont envoyés au premier module AS au moyen d'une première commande EXPORTKEY. De la même façon, la clef applicative TA chiffrée, le nombre REF2 relatif à une clef applicative TA, la signature SAS ainsi que le certificat CAS s'ils existent, sont envoyés au deuxième module EI au moyen d'une deuxième commande IMPORTKEY.

L'invention s'applique plus particulièrement dans le cas où le premier module AS de sécurité est une carte à puce. La carte à puce comprend un corps de carte plastique dans lequel est incorporé un module électronique comportant une puce à circuit intégré. Ladite puce comprend couramment deux mémoires M et une troisième mémoire volatile (RAM), la première mémoire M étant réinscriptible (EEPROM) et la deuxième non réinscriptible (ROM). La première mémoire M comprend l'ensemble des clefs applicatives TA. La troisième mémoire comprend la clef T1 d'exploitation; Celle-di ne demeure dans ladite mémoire que le temps de chiffrement ou de déchiffrement de la clef applicative selon le module de sécurité. La clef T de transport ainsi que les algorithmes ALGO1 de diversification et ALGO2 de cryptage peuvent se trouver dans la première mémoire M1 ou la deuxième mémoire M2. Cependant, on notera qu'il n'est pas obligatoire d'avoir lesdits algorithmes dans la carte à puce. Ils peuvent se trouver dans une entité extérieure à ladite carte à puce, par exemple dans une unité centrale d'un terminal avec lequel serait connectée ladite carte à puce.

La carte à puce permet d'assurer une meilleure protection des clefs applicatives TA. Dans une carte à puce, contrairement à un terminal d'un ordinateur par exemple, lesdites clefs sont inconnues de toute entité (d'un terminal, d'un utilisateur de ladite carte, d'une autre carte à puce, ...) excepté de l'entité émettrice desdites clefs. De plus, une fraude est plus difficile à réaliser sur une carte à puce que sur une unité centrale d'un terminal par exemple. Pour les mêmes raisons, le deuxième module de sécurité est une carte à puce.

REVENDICATIONS

1 - Procédé de chargement sécurisé d'une clef applicative (TA) à partir d'un premier module (AS) de sécurité d'une unité centrale vers un ou plusieurs deuxièmes modules (EI) de sécurité, lesdits premier et deuxièmes modules comprenant chacun au moins une mémoire (M), caractérisé en ce qu'il comporte les étapes selon lesquelles :

- lors de chaque chargement, on calcule dans le premier module (AS) une clef (T1) d'exploitation à partir d'une information propre au deuxième module (EI), d'une clef (T) de transport et d'un algorithme (ALGO1) de diversification, ladite clef (T) de transport se trouvant dans le premier module (AS) de sécurité,
- on chiffre dans le premier module (AS) la clef applicative (TA) à partir d'informations comprenant ladite clef (T1) d'exploitation et d'un algorithme (ALGO2) de cryptage,
- on envoie au deuxième module (EI) des données (DONNEES) comprenant la clef applicative (TA) chiffrée,
- lors de chaque chargement, on calcule dans le deuxième module (EI) la clef (T1) d'exploitation à partir de l'information propre au deuxième module (EI), de la clef (T) de transport et de l'algorithme (ALGO1) de diversification, ladite clef (T) de transport se trouvant dans le module (EI) de sécurité, ladite clef (T1) d'exploitation n'étant pas enregistrée dans la mémoire (M) dudit module,
- on déchiffre dans le deuxième module (EI) la clef applicative (TA) chiffrée, à partir d'informations comprenant ladite clef (T1) d'exploitation et d'un algorithme (ALGO2P) de décryptage inverse de l'algorithme (ALGO2) de cryptage.

2 - Procédé selon la revendication 1, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On envoie au premier module (AS) l'information propre au deuxième module (EI), préalablement au calcul dans le premier module (AS) de la clef (T1) d'exploitation.

3 - Procédé selon les revendications 1 ou 2, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On envoie au premier module (AS) un nombre aléatoire issu du deuxième module (EI), préalablement au chiffrement dans le premier module (AS) de la clef applicative (TA).

4 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On envoie au premier module (AS) une information relative à ladite clef applicative (TA), préalablement au chiffrement dans ledit module (AS) de la clef applicative (TA).

5 - Procédé selon la revendication 4, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On choisit la clef applicative (TA) à chiffrer à partir de l'information relative à ladite clef applicative (TA), préalablement au chiffrement dans le premier module (AS) de la clef applicative (TA).

6 - Procédé selon l'une des revendications précédentes, caractérisé en ce que le chiffrement d'une clef applicative (TA) destinée à un deuxième module (EI) est unique.

7 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On vérifie que les données (DONNEES) comprenant la clef applicative (TA) chiffrée sont intègres.

8 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On envoie au deuxième module (EI) une information relative à une clef applicative (TA), préalablement au déchiffrement dans ledit module (EI) de la clef applicative (TA) chiffrée.

9 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On enregistre dans le deuxième module (EI), après le déchiffrement de la clef applicative (TA) chiffrée, ladite clef (TA) dans ledit module (EI).

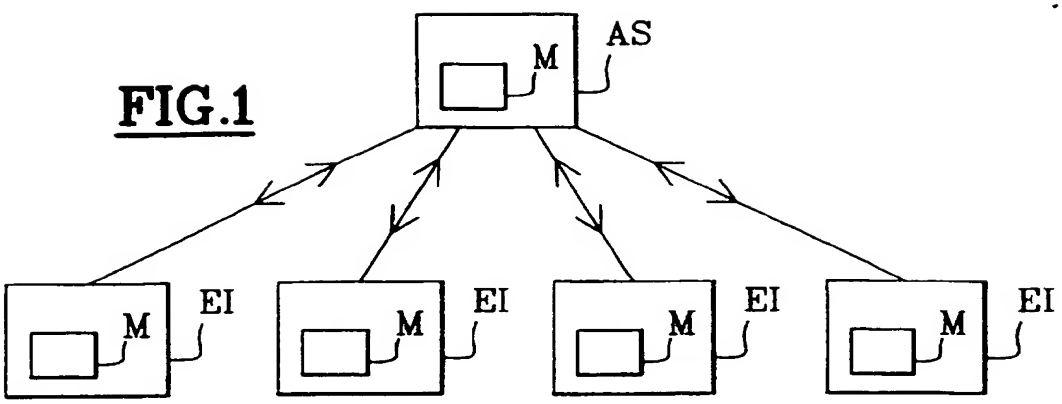
10 - Procédé selon la revendication 9, caractérisé en ce que l'enregistrement dans ledit deuxième module (EI) de la clef applicative (TA) se fait en fonction de l'information relative à une clef applicative (TA).

11 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On vérifie que la clef applicative (TA) est authentique.

12 - Procédé selon l'une des revendications précédentes, caractérisé en ce que le premier module de sécurité (AS) est une carte à puce.

FIG.1



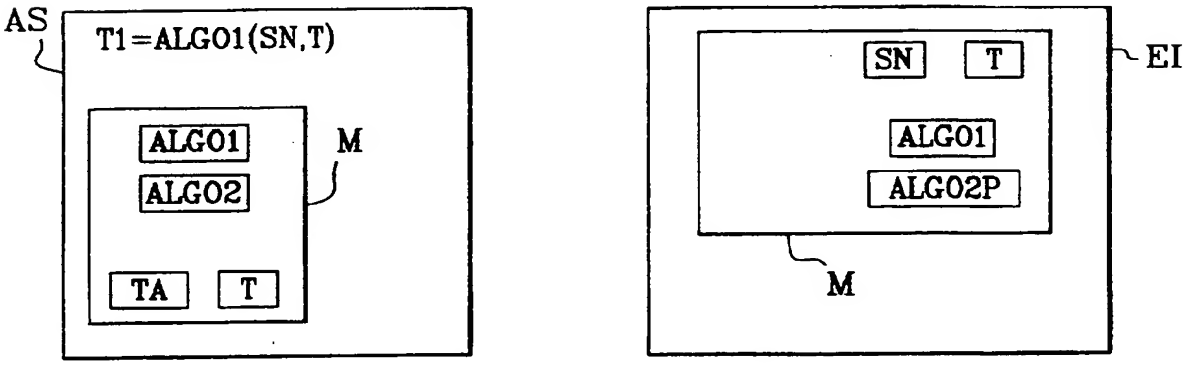


FIG.2

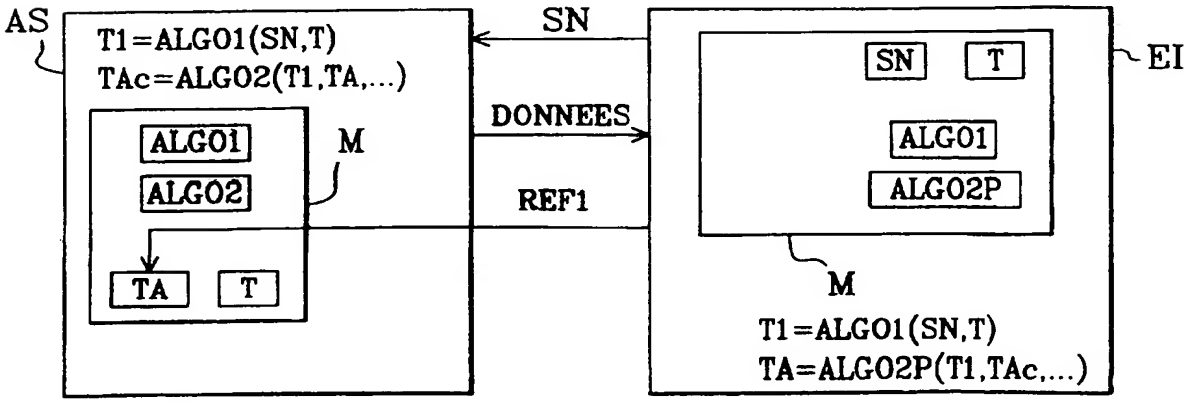


FIG.3

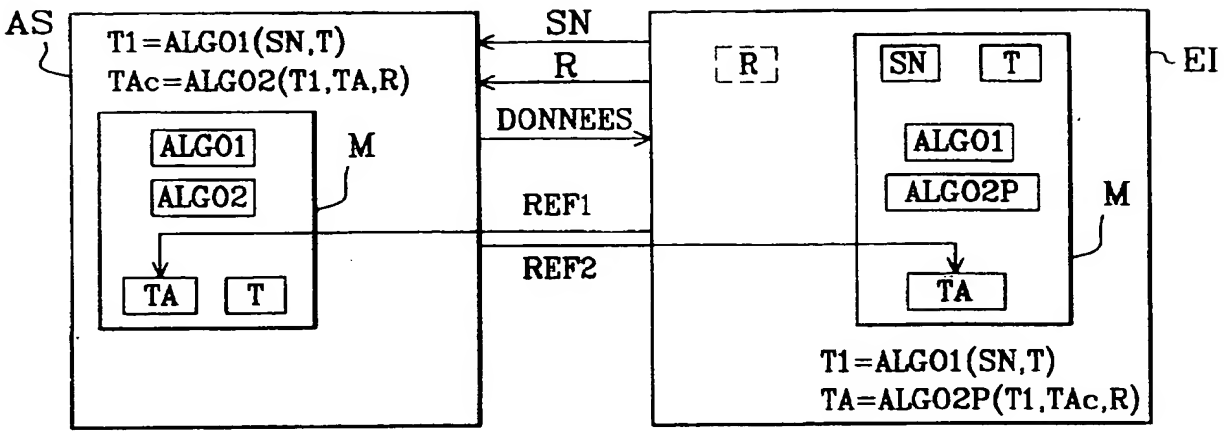

AS
T1=ALGO1(SN,T)
TAc=ALGO2(T1,TA,R)
ALGO1
ALGO2
M
TA
T
SN
R
DONNEES
REF1
REF2
R
SN
T
EI
ALGO1
ALGO2P
M
TA
T1=ALGO1(SN,T)
TA=ALGO2P(T1,TAc,R)

FIG.4

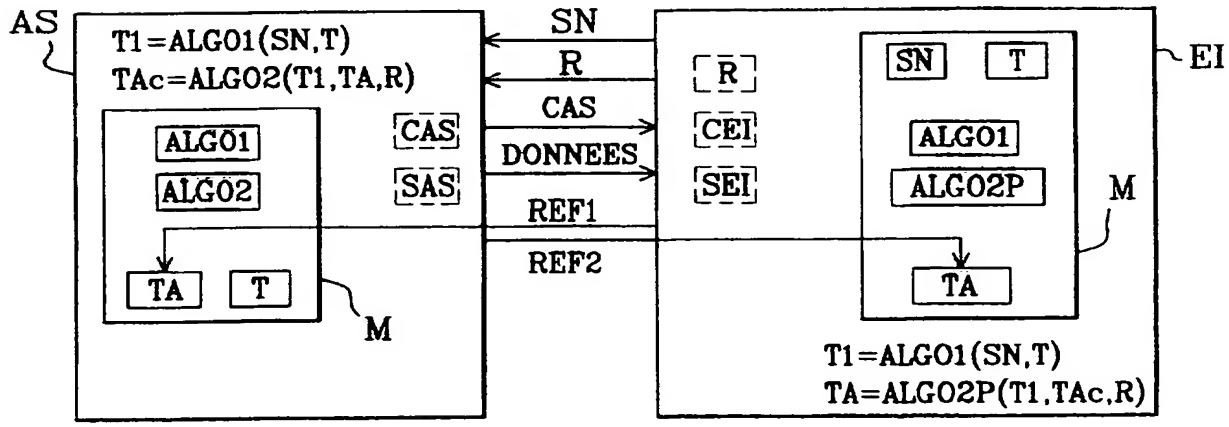

AS
T1=ALGO1(SN,T)
TAc=ALGO2(T1,TA,R)
ALGO1
ALGO2
CAS
SAS
TA
T
M
SN
R
CAS
DONNEES
REF1
REF2
R
CEI
SEI
SN
T
EI
ALGO1
ALGO2P
M
TA
T1=ALGO1(SN,T)
TA=ALGO2P(T1,TAc,R)

FIG.5

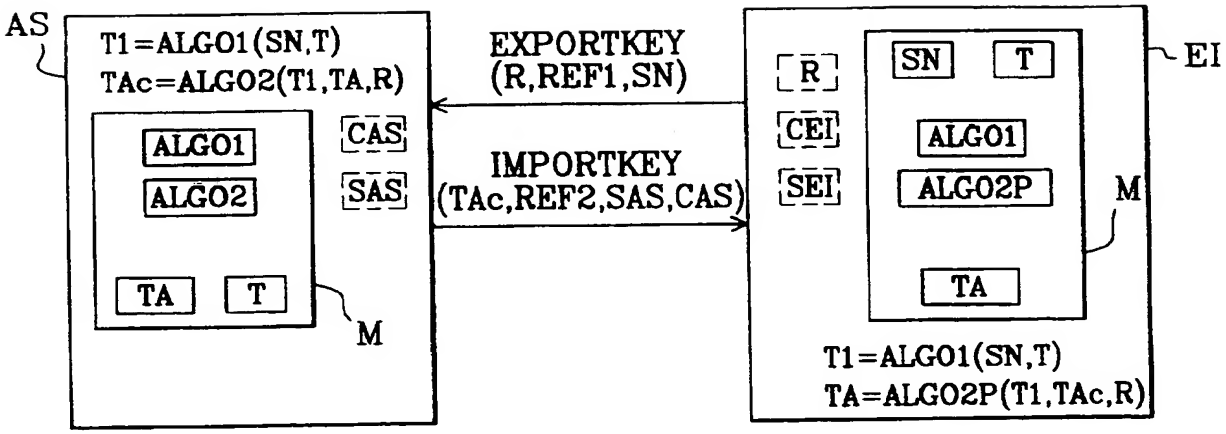

AS
T1=ALGO1(SN,T)
TAc=ALGO2(T1,TA,R)
ALGO1
ALGO2
CAS
SAS
TA
T
M
EXPORTKEY
(R,REF1,SN)
IMPORTKEY
(TAc,REF2,SAS,CAS)
R
CEI
SEI
SN
T
ALGO1
ALGO2P
TA
M
EI
T1=ALGO1(SN,T)
TA=ALGO2P(T1,TAc,R)

FIG.6

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2788649

N° d'enregistrement national

FA 570510
FR 9900462

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X	US 5 517 567 A (EPSTEIN PHILIP) 14 mai 1996 (1996-05-14) * colonne 5, ligne 55 - colonne 7, ligne 40 * * colonne 8, ligne 5 - ligne 10 *	1,3,6,9
A	FR 2 681 165 A (GEMPLUS CARD INT) 12 mars 1993 (1993-03-12) * page 5, ligne 17 - ligne 30 * * page 7, ligne 20 - page 10, ligne 18 *	1-3,6,9, 12
A	WO 97 24831 A (MCI COMMUNICATIONS CORP) 10 juillet 1997 (1997-07-10) * abrégé * * page 9, ligne 13 - ligne 23 *	1,4,5
A	WO 97 47109 A (SIEMENS AG ;EUCHNER MARTIN (DE); KESSLER VOLKER (DE)) 11 décembre 1997 (1997-12-11) * page 6, ligne 17 - ligne 22 * * page 12, ligne 29 - page 14, ligne 2 *	7,11
A	EP 0 688 929 A (NANOTEQ PTY LTD) 27 décembre 1995 (1995-12-27) * abrégé * * figure 1 *	1,7

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

H04L

Date d'achèvement de la recherche: 11 octobre 1999

Examinateur: Holper, G

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)